

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-325881

(43)公開日 平成9年(1997)12月16日

(51)Int.Cl.⁹

識別記号

庁内整理番号

F I

技術表示箇所

G 0 6 F 7/58

G 0 6 F 7/58

A

審査請求 有 請求項の数 5 O L (全 9 頁)

(21)出願番号

特願平8-142057

(22)出願日

平成8年(1996)6月5日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 島田 道雄

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 弁理士 ▲柳▼川 信

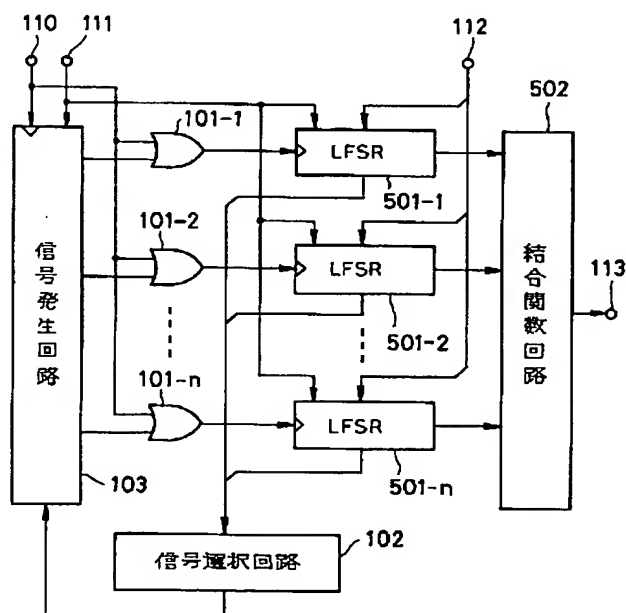
(54)【発明の名称】 擬似乱数発生装置

(57)【要約】

【課題】 複数のパルスから構成されるクロックの入力に応じて夫々シフト動作する n 個 (n は正の整数、以下同じ)のシフトレジスタと、この n 個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含む擬似乱数発生装置において、シフトレジスタの段数や個数を増加せずに、コリレーションアタックされにくいようにする。

【解決手段】 n 個のシフトレジスタに入力されるクロックのパルスを間引く。この場合、 n 個のシフトレジスタに同一時刻に入力されるパルスのうちの1つのみを間引く。

【効果】 一般的に用いられている4入力の結合関数回路を使っても、非線形性の高い擬似乱数を生成できる。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 複数のパルスから構成されるクロックの入力に応じて夫々シフト動作する n 個（ n は正の整数、以下同じ）のシフトレジスタと、この n 個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含む擬似乱数発生装置であって、前記 n 個のシフトレジスタに入力されるクロックのパルスを間引くクロック間引き手段を含むことを特徴とする擬似乱数発生装置。

【請求項2】 前記クロック間引き手段は、前記 n 個のシフトレジスタに同一時刻に入力されるパルスのうちの1つのみを間引くことを特徴とする請求項1記載の擬似乱数発生装置。

【請求項3】 前記結合関数回路は t 次（ t は正の整数、以下同じ）コリレーションイミュンであり、前記クロック間引き手段は長さ L （ L は正の整数、以下同じ）でハミング重みが $L \times t / n$ 以下の互いに異なる n 種類の2値系列をクロックとして前記 n 個のシフトレジスタに入力せしめ、前記シフトレジスタは入力される2値系列の値が“0”のときにシフト動作を行うことを特徴とする請求項1又は2記載の擬似乱数発生装置。

【請求項4】 前記シフトレジスタは、線形フィードバックシフトレジスタであることを特徴とする請求項1～3のいずれかに記載の擬似乱数発生装置。

【請求項5】 前記シフトレジスタは、非線形フィードバックシフトレジスタであることを特徴とする請求項1～3のいずれかに記載の擬似乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は擬似乱数発生装置に関し、特に通信システムや計算機システムにおいて採用され、許可されていない者が不正に情報を取得すること等を防止するために、情報に擬似乱数を排他的論理和で加算して暗号に変換したり暗号に擬似乱数を排他的論理和で加算して元の情報を復元するストリーム暗号装置等に用いられる擬似乱数発生装置に関する。

【0002】

【従来の技術】従来から広く知られている暗号として、ストリーム暗号と呼ばれるものがある。これは、擬似乱数発生装置によって生成される擬似乱数系列と、送信する情報系列との排他的論理和を、暗号系列として送信するものである。なお、一般的には、情報系列が“0000...”であっても不正解読ができないように、ストリーム暗号が設計される。情報系列が“0000...”の場合には、ストリーム暗号の出力する暗号系列から情報系列を不正解読することと、擬似乱数から擬似乱数発生装置の内部状態を推定することとは等価である。このため、以下では、「ストリーム暗号が不正解読されるという代わりに、単に「擬似乱数発生装置が不正解読される」ということもある。

【0003】また、従来から広く知られている擬似乱数発生装置として、複数の線形フィードバック・シフトレジスタ（Linear Feedback Shift Register；以下、LFSRと略す）の出力する擬似乱数を、結合関数と呼ばれる非線形関数によって非線形結合して、より非線形性の高い擬似乱数を生成する方法がある。ここで、非線形結合とは線形結合ではない結合のことであり、ビット x_1, \dots, x_n （ n は正の整数、以下同じ）の線形結合とは $y = x_1 + x_2 + \dots + x_n$ や $y = x_1 + x_2 + \dots + x_n + 1$ など、排他的論理和+だけを使ってビット y を与えることである。言い換えると、ビット x_1, \dots, x_n の非線形結合とは、 $y = x_1 * x_2 + x_2 * x_3 + \dots + x_n * x_1$ 等、論理積*と排他的論理和+との両方を使ってビット y を与えることであり、 y を与える式をどのように変形しても線形結合に帰着しないようなものである。また、非線形結合の非線形性とは、 y を与える式の次数のことであり、式の次数が大きいくほど非線形性が高いといわれる。なお、当然のことながら、結合関数の入力を増やせば増やすほど、非線形性の高い非線形結合が実現可能になる。

【0004】図6は、従来の擬似乱数発生装置の構成を示すブロック図である。図において、 n 個のLFSR501-1～501-nは、入力端子511に“0”が供給されているときには、入力端子510にパスが入力されると、入力端子512から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。なお、それぞれのLFSR501-1～501-nには、一般にはLFSR毎に異なった初期状態が供給される。また、LFSR501-1～501-nは、入力端子511に“1”が供給されているときには、入力端子510にパルスが1個入力される毎に、擬似乱数を出力する。 n 個のLFSR501-1～501-nの出力する擬似乱数は、結合関数回路502に入力され、結合関数回路502の出力が、擬似乱数として出力端子513から出力される。

【0005】なお、図6の擬似乱数発生装置に、擬似乱数を発生させるには、次のようにする。まず、入力端子512に初期状態を供給する。次に、入力端子511に“0”を供給して、入力端子510にパルス（あるいはクロックと呼ぶ）を1個入力する。そして、入力端子511に“1”を供給する。すると、それ以降は、入力端子510にパルスを1個入力する毎に、出力端子513から擬似乱数が得られる。

【0006】図7は、LFSR501-1～501-nを示す機能ブロック図である。図において、シフトレジスタ601は、入力端子611に“0”が供給されているときには、入力端子610にパルスが入力されると、入力端子612から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。また、シフトレジスタ601は、入力端子611に“1”が供給されてい

3

るときには、入力端子610にパルスが1個入力されると、保持されているビット系列を右側に1ビットだけシフトして、排他的論理和回路602の出力をビット系列の左端のビットとして保持する。なお、ビット系列の右端に保持されていたビットは、保持されているビット系列が右側に1ビットだけシフトされると、捨てられる。

【0007】また、シフトレジスタ601に保持されているビット系列は、出力端子613に供給されている。排他的論理和回路602は、シフトレジスタ601に保持されているビット系列のうち、予め決められた位置にあるビットの排他的論理和を計算して、計算結果をシフトレジスタ601に供給する。排他的論理和回路602の出力は、出力端子614にも供給されており、それが擬似乱数として出力される。LFSR501-1~501-nの構造は全て同一であるが、シフトレジスタ601の長さ、シフトレジスタ601に記憶されているビットのうち排他的論理和回路602に供給されるビットの位置は、一般に、LFSR毎に異なっている。なお、入力端子610、611、612には、それぞれ図6の入力端子510、511、512から入力される値が供給されており、出力端子614の出力は図6の結合関数502に供給されている。出力端子613の出力は、図6においては、使われていない。

【0008】結合関数回路502とは、入力されたビットの非線形結合をとってその結果を出力する結合関数の機能を持つものであり、論理関数回路やリード・オン・メモリ（ROM）あるいはそれらの組み合わせによって表現される。図8は、4入力の結合関数回路502の一例を示す機能ブロック図である。これは、 $n=4$ とした擬似乱数発生装置で使われるもので、4個のLFSR501-1~501-4の出力する擬似乱数が、それぞれ入力端子701-1~701-4に供給される。

【0009】論理積回路701は、入力端子710-1に供給される値と入力端子710-2に供給される値の論理積を計算して、その結果を出力する。論理積回路702は、入力端子710-1に供給される値と入力端子710-3に供給される値の論理積を計算して、その結果を出力する。論理積回路703は、入力端子710-2に供給される値と入力端子710-3に供給される値の論理積を計算して、その結果を出力する。排他的論理和回路704は、論理積回路701の出力と論理積回路702の出力と論理積回路703の出力と入力端子710-4に供給される値との排他的論理和を計算し、計算結果を出力端子711から出力する。出力端子711の出力は図6の出力端子513に供給されている。

【0010】しかしながら、従来の擬似乱数発生装置のLFSR501-1~501-nに与えられた初期状態は、しばしば、コリレーション・アタック（correlation attack）と呼ばれる解説方法で推定されてしまう。すなわち、あるLFSR501-j

4

（ $j=1\sim n$ ）の出力で条件付けたときの結合関数回路502の出力の条件付き確率分布が一樣でない場合には、そのLFSR501-jと等価なLFSRの出力系列と結合関数回路502の出力系列との相関を最大にするような等価LFSRの初期状態を総当りで求めることで、LFSR501-jに与えられた初期状態が求められてしまう。

【0011】また、一般的に、ある t 個のLFSRの出力で条件付けたときの結合関数回路502の出力の条件付き確率分布が一樣でない場合には、それらの t 個のLFSRと等価な t 個のLFSRの出力系列と結合関数回路502の出力系列との相関を最大にするような t 個の等価LFSRの初期状態を総当りで求めることで、 t 個のLFSRに与えられた初期状態が求められる。なお、以上の説明では、説明の便宜上、結合関数回路502の出力系列からLFSRの初期状態を推定することを考えたが、情報系列は理想的な乱数ではなく冗長度を持っているので、以上の操作において、結合関数回路502の出力系列の代わりに暗号系列を用いても、LFSRの初期状態を推定できる。すなわち、コリレーション・アタックは、情報系列が“0000...”でない場合でも、実行可能である。

【0012】なお、注意しておくが、何次までのコリレーション・アタックが実行できるか否かは、結合関数の性質だけでなく、 t 個のLFSRの段数の合計にも依存して決まる。例えば、 t 個のLFSRの段数の合計が64ビットであれば、求める初期状態を総当りで求めることが困難になるので、 t 次のコリレーション・アタックは実行できないが、 t 個のLFSRの段数の合計が20ビットであれば、 t 次のコリレーション・アタックは容易に実行できる。

【0013】このため、従来は、 $(t+1)$ 次のコリレーション・アタックが実行できなくなるほどLFSRの段数を増やすと共に、 t 個のLFSRの出力で条件付けたときの結合関数の出力の条件付き確率分布が一樣であるような結合関数を用いて、 t 次のコリレーション・アタックを防いでいた。なお、そのような結合関数は、 t 次コリレーション・イミュン（correlation immune）であると言われる。例えば、4入力の結合関数を用いる場合には、結合関数を1次コリレーション・イミュンにできることが知られているので、2次のコリレーション・アタックが実行できないようにLFSRの段数が選択される。なお、図6の4入力結合関数回路は、1次コリレーション・イミュンであることが知られている。

【0014】なお、従来の擬似乱数発生装置及びコリレーション・アタックや4入力結合関数に関しては、例えば、特開平7-104976号公報や、1986年にスプリング・ヴァーラグから刊行されたルエッペル著「アナリシス・アンド・デザイン・オブ・ストリーム・

5

サイファー」(R. A. Rueppel著 Analysis and Design of Stream Ciphers, Springer-Verlag, 1986)の第92頁から第141頁にかけてや、島田道雄著「結合関数の無相関性について」(第17回情報理論とその応用シンポジウム予稿集1994年)の第53頁から第56頁にかけて詳しい解説がある。

【0015】

【発明が解決しようとする課題】従来の擬似乱数発生装置の問題点は、上述した文献(島田道雄著「結合関数の無相関性について」)で示されているように、コリレーション・イミュンな結合関数を使っている、差分コリレーション・アタックで解読できるということである。その理由は、例えば、図6の4入力結合関数回路を考えてみれば分かる。図8の4入力結合関数回路の場合には、入力端子710-4の入力が線形結合している、入力端子710-4に擬似乱数を供給しているLFSRの周期をLとすると、時刻tと時刻L+tにおける結合関数の出力の差分をとることで、そのLFSRの出力の影響が結合関数の出力の差分に出なくなるようにすることができる。そうすると、4入力の結合関数に基づく擬似乱数発生装置を1次コリレーション・アタックで解読することが、3入力結合関数に基づく擬似乱数発生装置を1次コリレーション・アタックで解読することに帰着してしまう。3入力結合関数は、1次コリレーション・イミュンにできないので、1次コリレーション・アタックで簡単に解読されてしまう。

【0016】本発明は上述した従来技術の欠点を解決するためになされたものであり、その目的は、LFSRの段数や個数を増やさずに、LFSRに供給されるクロック信号を制御することで、ストリーム暗号に適した擬似乱数発生装置を提供することである。

【0017】

【課題を解決するための手段】本発明による擬似乱数発生装置は、複数のパルスから構成されるクロックの入力に応じて夫々シフト動作するn個(nは正の整数、以下同じ)のシフトレジスタと、このn個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含む擬似乱数発生装置であって、前記n個のシフトレジスタに入力されるクロックのパルスを間引くクロック間引き手段を含むことを特徴とする。

【0018】

【発明の実施の形態】本発明の作用は以下の通りである。

【0019】さて、良く考えてみると、コリレーション・アタックが成功するためには、次の2つの条件が必要であることが分かる。すなわち、第1の条件は、解読者が擬似乱数発生装置のLFSRと等価なLFSRを持っており、解読者が等価なLFSRの初期状態を適切に設

6

定することで、その等価LFSRに、擬似乱数発生装置のLFSRと同じ擬似乱数系列を発生させられるというものである。また、第2の条件は、既に述べたように、結合関数の入出力間に相関があるというものである。

【0020】これらの2つの条件が揃わないとコリレーション・アタックが実行できないのである。そして、従来は、第2の条件を崩すことで、すなわち、結合関数の入出力間に相関が出ないようにすることで、コリレーション・アタックを防いでいたのである。

【0021】そこで本発明では、第1の条件を崩すことで、コリレーション・アタックを防ぐことにした。すなわち、従来の擬似乱数発生装置では、それぞれのLFSRに常にクロック信号を供給していたのだが、本発明では、クロックのパルスを間引いてクロック信号のパターンを変化させることにした。すなわち、従来は、“0000・・・”というクロック信号を使っていたのに対して、本発明では、それ以外の2値系列もクロック信号として使用することにした。クロック信号のパターンを解読者に秘密にしておけば、複製されたLFSRに擬似乱数発生装置のLFSRと同じ擬似乱数発生系列を発生させられないので、第1の条件が崩れ、コリレーション・アタックが実行できなくなる。

【0022】なお、以上では、クロック信号を2値系列として表現したが、2値系列のτ番目が“0”であるということは、クロック信号のτ単位時刻にパルスが有ることを意味し、2値系列のτ番目が“1”であることは、クロック信号のτ単位時刻にパルスが無いことを意味する(“0”と“1”とを入れ替えても良いのだが、説明の便宜上、このようにしておく)。また、単位時刻とは、クロック信号の周期すなわちパルス1個の長さに相当する時刻を“1”として測った時間のことである。

【0023】ただし、ただ単にランダムにクロック信号のパターンを選択するのでは、擬似乱数発生装置の出力する擬似乱数の周期が極端に短くなる危険性がある。例えば、どのLFSRも周期Tビットの周期系列を擬似乱数系列として出力したら、擬似乱数発生装置の出力する擬似乱数系列も周期Tビットの周期系列になってしまう。擬似乱数系列の周期が短いと、例えば、盗聴によって得られた擬似乱数系列全体をメモリに記憶しておき、それを暗号系列に排他的論理和で加算することで、簡単に不正解読されてしまう。

【0024】そこで本発明では、次のような工夫によって、擬似乱数の周期が短くなることを防いでいる。すなわち、クロック信号として、互いに長さnとハミング重みとが等しいn個の2値系列から構成されるn個組を、予め複数個選んでおき、それら複数個のn個組みからランダムに1つのn個組を選択し、選択されたn個組みの各2値系列を、n個のLFSRのそれぞれに逐次的に供給する。例えば、n=4の場合には、次のようにする。

【0025】まず、4個組みとして、(0001, 00

10, 0100, 1000) (4単位時刻分), (1000, 0100, 0010, 0001), (4単位時刻分) (0, 0, 0, 0) (1単位時刻分)を用意しておく。そして、ある時刻に1番目の4個組みが選択されたならば、その4個組みの2値系列の長さは“4”であるから、次の4単位時刻までは、LFSR501-1には、“0001”を、LFSR501-2には“0010”を、LFSR501-3には“0100”を、LFSR501-4には“1000”をそれぞれクロック信号として供給する。すると、“1”の場合にクロックパルスが間引かれ、次の4単位時刻後までには、どのLFSRにも3個のパルスが供給されることになる。このことは、結果だけを見れば、どのLFSRにも“000”というクロック信号が供給されたのと等価である。つまり、“0”の場合にはLFSRはシフト動作を行い、“1”の場合にシフト動作を行わない。また、各LFSRに供給されるクロック信号の“1”の位置が互いに異なるので、各LFSRに同一時刻に入力されるパルスのうちの1つのみを間引くことになる。

【0026】以上のようにすれば、本擬似乱数発生装置のLFSRの内部状態が、少なくとも特定の時刻においては、従来の擬似乱数発生装置のLFSRの内部状態と同様に推移する。このため、擬似乱数発生装置の出力する擬似乱数系列の周期が擬似乱数発生装置の出力する擬似乱数発生系列の周期よりも短くなることはない。

【0027】ただし、ただ単にクロック信号として、互いに長さハミング重みとが等しい2値系列から構成されるn個組を用いるのでは、依然として、簡単に不正解読される危険性がある。なぜなら、前述の例において、例えば、ハミング重みが“3”である(1110, 1101, 1011, 0111)という2値系列の4個組みを用いると、ある時刻に出力された擬似乱数と次の時刻に出力された擬似乱数との間に相関が生じることがあるからである。すなわち、4入力の結合関数は高々1次コリレーション・イミュンであり、クロック信号のハミング重みが“3”であれば、ある時刻と次の時刻とでは3個のLFSRの出力が等しくなることがあるからである。

【0028】そこで、本発明では、結合関数がt次コリレーション・イミュンであれば、長さLのクロック信号として、ハミング重みが Lt/n であるような2値系列だけを使用する。例えば、 $n=4$ の場合には、結合関数が1次コリレーション・イミュンであれば、長さ“4”のクロック信号として、ハミング重みが“1”であるような、“0001”, “0010”, “0100”, “1000”といった“1”の位置が互いに異なる2値系列だけを、n個組みの要素として使用するのである。そのようにすれば、ある時刻と次の時刻とで出力が常に等しいのは1個のLFSRだけになるから、1次コリレーション・イミュンな結合関数を使うことで、

ある時刻に出力された擬似乱数と次の時刻に出力された擬似乱数との間に相関が生じることを防ぐことができる。

【0029】次に、本発明の実施例について図面を参照して詳細に説明する。

【0030】図1は、本発明の擬似乱数発生装置の一実施例の構成を示すブロック図であり、図6と同等部分は同一符号により示されている。

【0031】図において、本実施例の擬似乱数発生装置は、クロックが入力されるごとに1ビットの擬似乱数を生成するn個のLFSR501-1~501-nと、これらn個のLFSRの出力する擬似乱数を非線形結合してビットを生成するt次コリレーション・イミュンな結合関数回路と、n個のLFSRに記憶されたビットのうち予め決められた一部又は全部のビットに予め決められた非線形変換を施して予め決められた個数のビットを出力する信号選択回路102と、信号選択回路102の出力に依存して、長さがLでハミング重みが Lt/n 以下であるようなn個の2値系列を、外部から入力されるクロックに同期して逐次に出力する信号発生回路103と、外部から入力されるクロックと信号発生回路103の出力との論理和を演算して、その演算結果をn個のLFSRにクロックとして供給するn個の論理和回路101-1~101-nとを含んで構成され、外部から入力されるクロックに同期して結合関数回路502より擬似乱数を出力する。

【0032】LFSR501-1~501-nは、入力端子111に“0”が供給されているときには、論理和回路101-1~101-nからパルスが供給されると、入力端子112から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。また、LFSR501-1~501-nは、入力端子111に“1”が供給されているときには、論理和回路101-1~101-nからパルスが供給されるごとに、内部状態を更新すると共に擬似乱数を出力する。そして、LFSR501-1~501-nの出力する擬似乱数が、結合関数回路502に入力されて、結合関数回路502の出力が、擬似乱数として出力端子113から出力される。LFSR501-1~501-nの内部状態は、信号選択回路102に供給されている。なお、LFSR501-1~501-nの内部状態は、図7の出力端子613を介して出力される。

【0033】信号選択回路102については、後で詳しく述べるが、LFSR501-1~501-nの内部状態に対して予め決められた非線形変換を施して、予め決められた数のビットを発生する。信号発生回路103については、後で詳しく述べるが、信号選択回路102の出力に応じて、予め決められたクロック信号を生成して、論理和回路101-1~101-nに供給する。論理和回路101-1~101-nは、入力端子110か

ら供給されるパルス系列と、信号発生回路103から供給されるクロック信号との論理和をとることで、クロック信号に対応するパルス系列を生成して、そのパルス系列を、それぞれLFSR501-1~501-nに供給する。

【0034】なお、図1の擬似乱数発生装置に擬似乱数を発生させるには、次のようにする。まず、入力端子112に初期状態を供給する。次に、入力端子111に“0”を供給して、入力端子110にパルスを1個入力する。そして、入力端子111に“1”を供給する。すると、それ以降は、入力端子110にパルスを1個入力するごとに、出力端子113から擬似乱数が得られる。

【0035】図2は、 $n=4$ とする図1の擬似乱数発生装置で使われる信号選択回路102の基本構成の一例を示す機能ブロック図である。図において、図1のLFSR501-1~501-4の出力が、それぞれ入力端子210-1~210-4に供給されている。配線201は、予め決められた配線であり、入力端子210-1~210-4から供給される信号の予め決められた一部あるいは全部を、重複も許して出力する。配線201の出力は、 u 個（ u は正の整数、以下同じ）の論理積回路202-1~202- u の出力は配線203に供給される。

【0036】配線203は予め決められた配線であり、論理積回路202-1~202- u から供給される信号の予め決められた一部あるいは全部を、重複も許して出力する。配線203の出力は、5個の排他的論理和回路204-1~204-5に供給され、排他的論理和回路204-1~204-5の出力は出力端子211から出力される。そして、出力端子211の出力が、図1の信号発生回路103に供給される。信号選択回路102の出力は、LFSR501-1~501-4の出力に依存しているので、LFSR501-1~501-4の全ての初期状態を知らない第三者は、信号選択回路102の出力を容易には推定できない。

【0037】図3は、 $n=4$ とする図1の擬似乱数発生回路で用いられる信号発生回路103の基本構成の一例を示す機能ブロック図である。図において、図1の入力端子110から入力される信号が入力端子320に供給され、図1の入力端子111から入力される信号が入力端子321に供給され、図1の信号選択回路102の出力が入力端子322に供給されている。カウンタ307は、入力端子321に“0”が供給されているときには、論理和回路302からパルスが供給されると、カウント値をゼロにする。また、カウンタ307は、入力端子321に“1”が供給されているときには、論理和回路302からパルスが供給されるごとに、カウント値を“1”だけ増加し、また、保持されているカウント値を、論理和回路306とデコーダ309とに供給する。なお、カウント値が3から“1”だけ増加したときに

は、カウント値は“0”に戻るものとする。

【0038】レジスタ308は、論理和回路301からパルスが供給されると、入力端子322に供給されている5ビットを保持し、また、保持されている5ビットのうち、左端のビットを論理和回路306に供給し、それ以外の4ビットを転置回路310に供給する。デコーダ309は、カウンタ307の出力が“x”であれば、右から“x”ビット目が1であるような4ビットを出力する。すなわち、デコーダ309は、 $x=“0”$ 、

“1”、“2”、“3”に対して、それぞれ“0001”、“0010”、“0100”、“1000”を出力する。転置回路310は、レジスタ308の出力に応じて、デコーダ309の出力ビットの転置（すなわち位置を入れ替えたもの）を出力する。なお、こういった転置を行うかは、予め決められているものとする。

【0039】セクタ311は、論理積回路304の出力が“0”であれば、転置回路310の出力を選択して出力し、論理積回路304の出力が“1”であれば、

“0000”を出力する。そして、セクタ311の出力が出力端子323から出力される。なお、出力端子323の出力は、図1の論理和回路101-1~101-5に供給される。

【0040】論理和回路306は、カウンタ307の出力とレジスタ308の出力の左端ビットとの計3ビットの論理和を計算して、その結果を出力する。否定回路305は、論理和回路306の出力を反転して、その結果を出力する。論理積回路303は、入力端子321から供給される信号と論理和回路306の出力の論理積を計算して、その結果を出力する。論理積回路304は、入力端子321から供給される信号と否定回路305の出力との論理積を計算して、その結果を出力する。論理和回路301は、入力端子320から供給される信号と論理積回路303の出力との論理和を計算して、その結果を出力する。論理和回路302は、入力端子320から供給される信号と論理積回路304の出力との論理和を計算して、その結果を出力する。

【0041】同図の信号発生回路の動作を説明すると、次のようになる。入力端子321に“0”が供給されているときに、入力端子320にパルスが供給されると、カウンタ307のカウント値が“0”に設定されると共に、入力端子322に供給されている5ビットがレジスタ308に保持される。そして、入力端子321に“1”が供給されており、かつ、カウンタ307のカウント値が“0”であり、かつ、レジスタ308に保持されている5ビットの左端のビットが“0”であれば、セクタ311から“0000”が出力され、入力端子320にパルスが1個入力されると、レジスタ308には入力端子322から供給される新しい5ビットが保持される。一方、入力端子321に“1”が供給されており、かつ、カウンタ307のカウント値が“0”であ

り、かつ、レジスタ 308 に保持されている 5 ビットの左端のビットが “1” であれば、次の 4 単位時刻後にカウンタ 307 のカウント値が再び “0” になるまで、出力端子 323 からハミング重みが “1” であるような 4 ビットが出力される。

【0042】図 4 は、 $n=4$ とする図 3 の信号発生回路 103 で用いられる転置回路 310 の基本構成の一例を示す機能ブロック図である。図において、入力端子 410-1~410-4 には、図 3 のデコーダ 309 の出力が供給され、入力端子 411 には、図 3 のレジスタ 308 の出力の右 4 ビットが供給されている。入力端子 410-1~410-4 に供給された信号は、配線 401-1 に入力される。配線 401-j ($j=1, 2, 3, 4$) は、4 ビットの入力に対して予め決められた 2 通りの配線によって、予め決められた互いに異なる 2 通りの転置を施す。そして、夫々の転置結果を図中の左側と右側とに出力し、夫々セクタ 402-j の左側と右側とに供給する。

【0043】セクタ 402-j ($j=1, 2, 3, 4$) には、入力端子 411 に供給されている 4 ビットのうち 1 ビットが供給されており、そのビットの値に応じて、左側あるいは右側の入力を選択して出力する。そして、セクタ 402-j ($j=1, 2, 3$) の出力は、配線 401-($j+1$) に入力され、セクタ 402-4 の出力は、出力端子 412-1~412-4 から出力される。なお、出力端子 412-1~412-4 から出力された 4 ビットは、図 3 のセクタ 311 の左側の入力に供給される。

【0044】ところで、図 1 中の線形フィードバックシフトレジスタ 501-1~501-n に代えて、非線形フィードバックシフトレジスタを用いても良い。図 5 は、非線形フィードバックシフトレジスタの一構成例を示すブロック図である。図において、シフトレジスタ 801 は、図 7 の LFSR 501 と同様の構造を持つものである。図中のシフトレジスタ 801 は、入力端子 811 に “0” が供給されているときに、入力端子 810 にパルスが入力されると、入力端子 812 から供給される初期状態と呼ばれるビット系列を、内部状態として保持する。また、シフトレジスタ 801 は、入力端子 811 に “1” が供給されているときに、入力端子 810 にパルスが 1 個入力されると、保持されているビット系列を右側に 1 ビットだけシフトして、排他的論理和回路 802 の出力をビット系列の左端のビットとして保持する。なお、ビット系列の右端に保持されていたビットは、保持されているビット系列が右側に 1 ビットだけシフトされると、捨てられる。

【0045】また、シフトレジスタ 801 に保持されているビット系列は、出力端子 813 と非線形関数回路 803 に供給されている。排他的論理和回路 802 は、シフトレジスタ 801 に保持されているビット系列のう

ち、予め決められた位置にあるビットの排他的論理和を計算して、計算結果をシフトレジスタ 801 に供給する。非線形関数回路 803 は、シフトレジスタ 801 に保持されているビット系列のうち、予め決められた位置にあるビットの非線形結合を計算する。すなわち、予め決められた位置にあるビットに対して、予め決められた排他的論理和以外の論理演算を施す。そして、その計算結果が擬似乱数として出力端子 814 から出力される。

【0046】要するに、線形フィードバックシフトレジスタの代わりに、非線形フィードバックレジスタを用いて擬似乱数発生装置を構成した場合でもクロックパルスを間引くことによってシフトレジスタの段数や個数を増やさずに、ストリーム暗号化に適した擬似乱数を発生することができるのである。

【0047】以上のように、本装置を用いて擬似乱数を発生させれば、全ての LFSR の初期状態を知らない第三者には、LFSR の内部状態がどのようなタイミングで推移しているか推測できないので、一般的に用いられている 4 入力の結合関数回路を使っても、コリレーション・アタック及び差分コリレーション・アタックに強い擬似乱数を発生できるのである。これにより、比較的簡単な構成でありながら、ストリーム暗号に適した擬似乱数発生装置が実現できる。

【0048】また、本装置では、結合関数回路において非線形な変換が行われるだけでなく、信号選択回路においても非線形な変換が行われ、その変換結果にも依存して擬似乱数が生成されるので、一般的に用いられている 4 入力の結合関数回路を使っても、非線形性の高い擬似乱数を生成できるのである。これにより、ストリーム暗号に適した擬似乱数発生装置が実現できる。

【0049】要するに本装置では、複数のパルスから構成されるクロックの入力に応じて夫々シフト動作する n 個のシフトレジスタと、この n 個のシフトレジスタの各出力を結合して擬似乱数を生成する結合関数回路とを含み、 n 個のシフトレジスタに入力されるクロックのパルスを間引いているのである。これにより、比較的簡単な構成でありながら、ストリーム暗号に適した擬似乱数を発生することができるのである。

【0050】

【発明の効果】以上説明したように本発明は、擬似乱数を発生する線形（非線形）フィードバックシフトレジスタへの入力クロックを間引くことにより、そのレジスタの初期状態を知らない第三者にはシフトレジスタの内部状態がどのようなタイミングで推移しているのか推測できず、比較的簡単な回路構成でコリレーション・アタックに強い擬似乱数を発生することができるという効果がある。

【図面の簡単な説明】

【図 1】本発明の実施例による擬似乱数発生装置の構成を示すブロック図である。

【図2】図1中の信号選択回路の内部構成例を示すブロック図である。

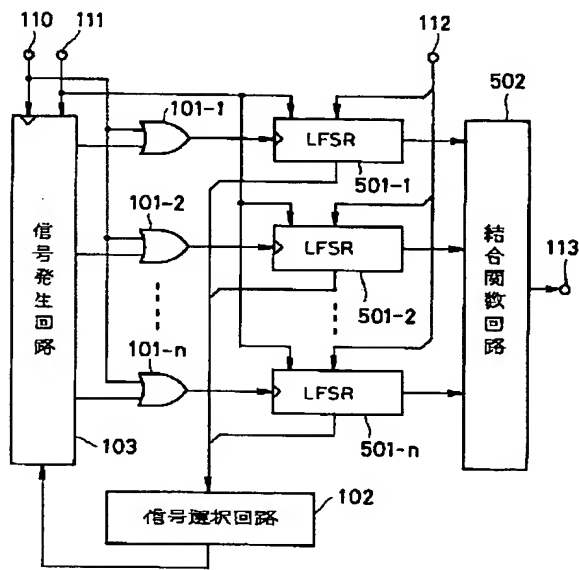
【図3】図1中の信号発生回路の内部構成例を示すブロック図である。

【図4】図3中の転置回路の内部構成例を示すブロック図である。

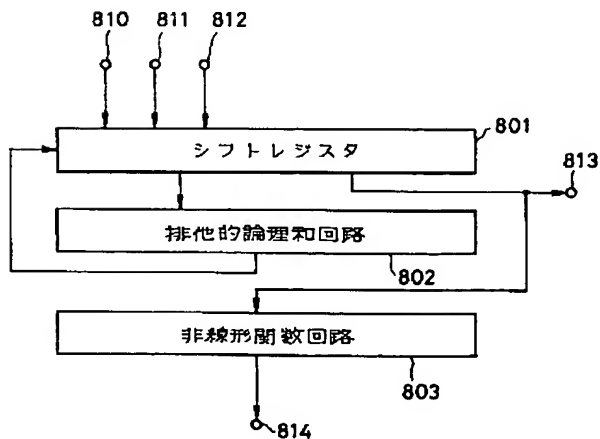
【図5】図1中のLFSRの代わりに用いる非線形フィードバックレジスタの内部構成例を示すブロック図である。

【図6】従来の擬似乱数発生装置の構成を示すブロック図である。

【図1】



【図5】



図である。

【図7】図6中のLFSRの内部構成例を示すブロック図である。

【図8】図6中の結合関数回路の内部構成例を示すブロック図である。

【符号の説明】

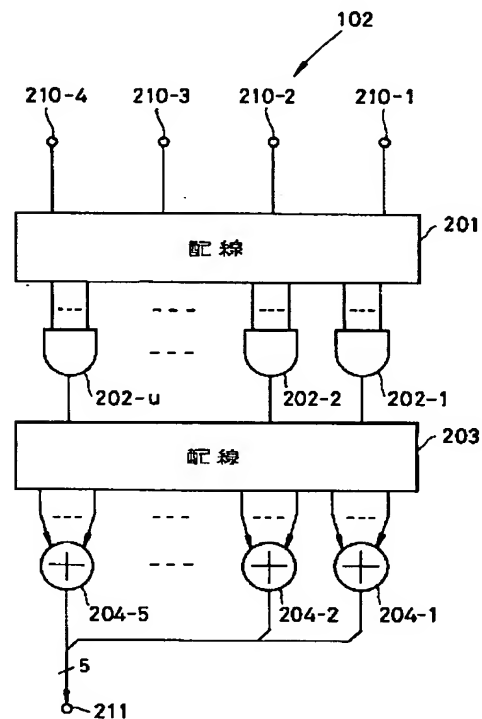
102 信号選択回路

103 信号発生回路

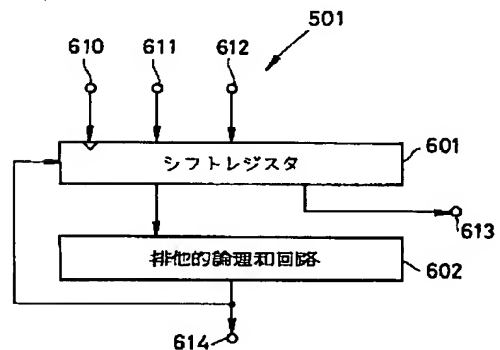
501-1~501-n LFSR

502 結合関数回路

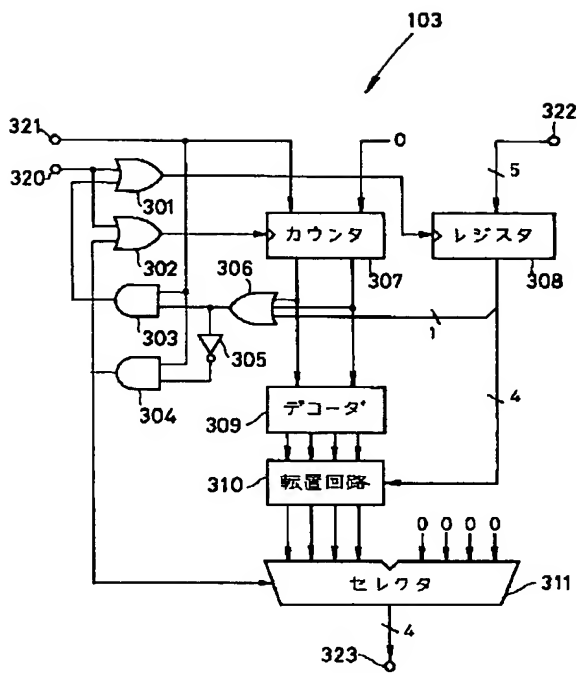
【図2】



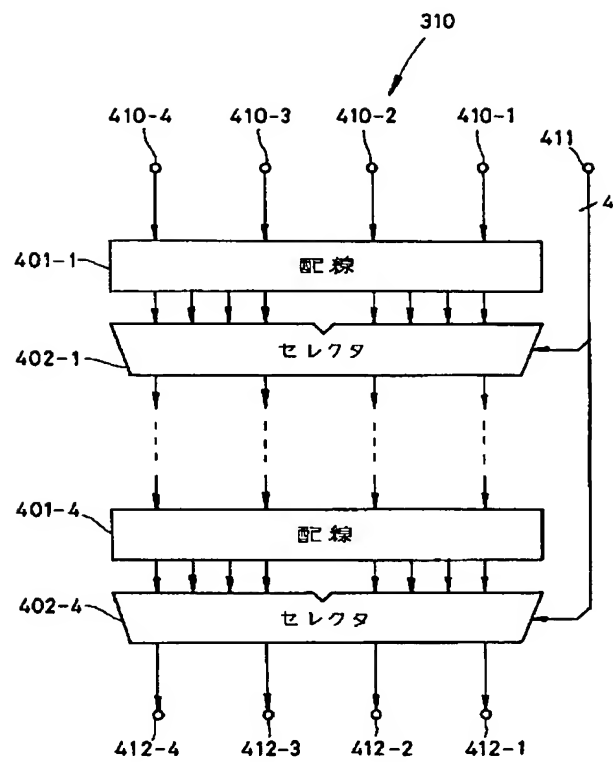
【図7】



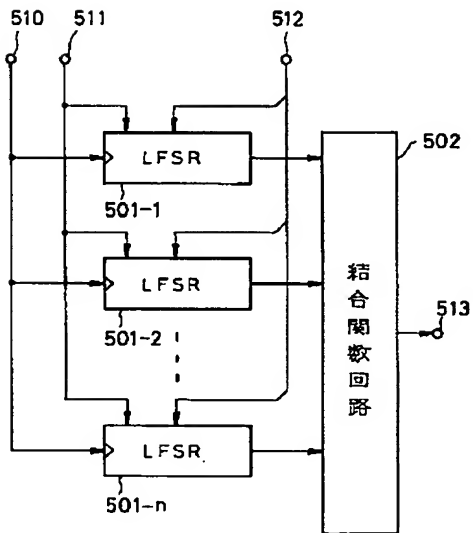
【図3】



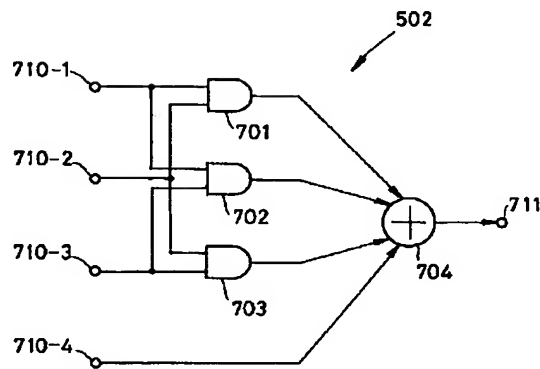
【図4】



【図6】



【図8】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.